NZ Incident Response Bulletin

Standard Edition –April 2026 – Issue #87

The NZ Incident Response Bulletin is a monthly high-level executive summary containing some of the most important news articles that have been published on Forensic and Cyber Security matters during the last month. Each Bulletin also includes a section of our own content, based on a trending theme. We'll give you a brief summary of each article, and a link to more information. Why do we publish this bulletin? Because we want to keep you up to date with the latest Forensic and Cyber Security news, so that you aren't caught by surprise – and you'll know about risks and changes before they become problems.

News:

A high-level executive summary containing some of the most important news articles that have been published on Forensic and Cyber Security matters during the last month.

New Zealand

Spy agency warns NZ's cyber security barely up to scratch

New Zealand's cyber security posture is being described as only marginally adequate in key areas, with the country's intelligence and cyber defence leadership warning that some parts of critical infrastructure are barely meeting acceptable standards. The concern comes as the Government introduces a refreshed national cyber security strategy and action plan, designed to modernise its approach in response to a more aggressive threat environment, growing supply chain exposure, and the added complexity created by technologies such as generative AI. Recent breaches affecting healthcare-related platforms including MediMap and Manage My Health are cited as practical examples of how weak controls can disrupt services and expose sensitive information. International incidents such as the Optus breach and the Colonial Pipeline ransomware attack also underline how cyber incidents can quickly become national economic and public confidence issues. For senior leaders, the central implication is that cyber resilience must be treated as a board-level business risk tied directly to operational continuity, regulatory pressure, and organisational trust.

NZ spy agency providing Iran war threat intelligence

New Zealand's Government Communications Security Bureau says it is supplying continuous threat intelligence updates in response to the Iran conflict, with a particular focus on supporting the New Zealand Defence Force and the Ministry of Foreign Affairs and Trade. The briefing reflects how quickly geopolitical crises can create national security and operational pressures for New Zealand, even when events occur far from home. Intelligence leaders told Parliament that the environment is highly volatile and that both the GCSB and SIS are taking a more proactive approach to detecting and disrupting threats, including those linked to foreign states, terrorism, cyber activity, and organised crime. The report also highlights the sensitivity of intelligence sharing within the Five Eyes partnership, with agency leaders stressing that New Zealand retains legal, policy, and human rights controls over what it shares and can withhold information where required. For executives, the wider implication is that international conflict can rapidly raise cyber, security, and continuity risks, reinforcing the need for strong situational awareness, trusted intelligence channels, and clear governance over crisis response.

Australia

Australian hospitals on alert after Iranian hackers attack medical technology company Stryker

Australian hospitals were placed on alert after the Iranian-linked Handala group claimed responsibility for a cyber attack on Stryker, the US medical technology company that supplies surgical and hospital equipment into Australia. While health officials in Victoria and New South Wales said there had been no direct service disruption at the time, the incident raised concerns about supply chain exposure and the broader risk of geopolitical conflict spilling into healthcare operations. Handala claimed to have wiped large volumes of systems and stolen significant data, although Stryker said the attack had been contained, customer and product environments were safe, and the impact was limited to its internal Microsoft environment. Security specialists warned that even without direct ransomware or malware spreading into hospitals, a prolonged outage could affect the availability of implants, consumables, and other essential equipment. The wider implication is that internationally connected suppliers can become indirect points of failure for healthcare providers, particularly when nation-state or state-aligned actors use cyber operations to advance political and military objectives.

Government entities in Queensland unaware of cybersecurity vulnerabilities, audit office report finds

A Queensland Audit Office review found serious weaknesses in how public sector entities manage third-party cyber risk, including cases where auditors were able to obtain passwords, access systems, extract sensitive information, and in two instances gain the highest level of access to IT environments. The findings show that some government bodies did not understand how exposed they were to supplier and partner vulnerabilities, despite third-party risk having been flagged for years. Contract management emerged as a major weakness, with only two of 36 contracts reviewed requiring third parties to report cyber incidents or vulnerabilities, leaving entities potentially blind to significant risks in their supply chain. The report also found that government efforts to build a consistent framework for managing third-party cyber risk have been slow, even though the threat environment has become more frequent and sophisticated. The recommended response includes updating IT systems, improving detection of suspicious activity, and strengthening governance and contractual controls, with smaller councils likely to face resourcing and capability challenges in implementing these changes.

World

Global cybercrime crackdown: over 373 000 dark web sites shut down

Europol's March announcement on a multinational crackdown against dark web infrastructure is notable because it demonstrates the scale and persistence of coordinated law enforcement action against cyber-enabled criminal ecosystems. Europol said the operation involved authorities from 23 countries and resulted in more than 373,000 dark web sites being shut down. For executives, the bigger story is not only the enforcement numbers, but what they reveal about the industrialisation of cybercrime. Dark web marketplaces, leak sites, and related infrastructure are not fringe phenomena. They are operating environments that support fraud, stolen data trade, malware services, and criminal collaboration at international scale. When authorities dismantle parts of that infrastructure, it may temporarily disrupt criminal operations, but it can also drive migration, fragmentation, and retaliation elsewhere in the ecosystem. Organisations should therefore view these takedowns as useful but not decisive victories. The more durable lesson is that cybercrime is a mature transnational market, and resilience depends on strong internal controls rather than assuming law enforcement pressure alone will reduce exposure.

EU sanctions Chinese and Iranian companies for cyberattacks

The European Union's decision to sanction two China-based companies and one Iranian company for cyberattacks is significant because it shows cyber activity being treated not just as a technical or intelligence problem, but as a matter of economic statecraft. Reuters reported that the measures targeted Integrity Technology Group, Anxun Information Technology, and Emennet Pasargad, with the EU linking them to attacks on member states and related disruptive activity. For executives, the main implication is that cyber risk is becoming more directly entangled with sanctions exposure, supply chain screening, and geopolitical compliance. Boards should expect greater scrutiny of vendor relationships, technology sourcing, due diligence processes, and any commercial dependencies that could intersect with sanctioned entities or politically sensitive cyber operations. This also reinforces that attribution, once seen as uncertain and mostly symbolic, is increasingly feeding into real policy action. Cyber events can now escalate into legal, financial, and operational issues even for organisations that are not the original target.

Companies House suspends online filing after glitch put personal data at risk

Companies House was forced to suspend its online WebFiling service after a software flaw exposed confidential personal details of company directors and created the risk that unauthorised users could alter company records. Reported exposures included directors' addresses, email addresses, and dates of birth, affecting records tied to more than 5 million UK companies, including major listed businesses. The flaw was reportedly simple enough to exploit through normal browser behaviour, which raised immediate concerns about fraud, impersonation, and the integrity of the UK corporate register. The incident is especially significant because Companies House has recently been given broader powers and a stronger mandate to improve trust in company data and prevent abuse of the registry. A later official update said passwords and identity verification documents such as passport data were not compromised, and that the issue was not believed to allow large-scale or systematic extraction of records. Even so, the event highlights how basic application weaknesses in public-facing systems can create outsized governance, privacy, and confidence risks.

New LexisNexis Data Breach Confirmed After Hackers Leak Files

LexisNexis has confirmed that attackers gained access to a limited number of servers after a threat actor leaked about 2GB of allegedly stolen data online. The company said the affected systems mainly contained legacy, deprecated data from before 2020, including customer names, user IDs, business contact information, survey respondent IP addresses, and support tickets, and that it has found no evidence that products or services were impacted. LexisNexis also said the exposed information did not include Social Security numbers, driver's licence numbers, financial data, active passwords, customer contracts, or client and matter information. The attackers, identified in reporting as FulcrumSec, claimed they exploited the React2Shell vulnerability and weakly secured AWS resources to obtain millions of records, including enterprise account data, employee credentials, and information tied to roughly 400,000 individuals. The incident highlights the continuing risk posed by legacy environments and over-privileged cloud access, especially where older data stores remain connected to modern infrastructure and can still create reputational, regulatory, and customer trust consequences when compromised.

Summary of last month's Cyber Alerts and News Clips:

Incident Response Solutions post certain alerts and tips we consider to be in the public interest as it comes to hand. We publish these alerts and tips on this webpage.

24/03/2026 – CVE-2026-20963 affecting SharePoint Server

Our Views:

Local AI Agents Move to the Endpoint – A New Cyber Risk Frontier

Recent advances in artificial intelligence are shifting capability from cloud-hosted platforms to tools that run directly on user devices. While this promises performance, privacy, and autonomy benefits, it also introduces a materially different cyber risk profile that many organisations are not yet prepared for.

Recent advances in artificial intelligence are shifting capability from cloud-based tools to software that runs directly on laptops and desktops. This brings clear benefits around speed and control, but it also introduces a different kind of cyber risk that many organisations are not yet factoring in.

What's Changed

A new generation of AI tools can now act more like a digital assistant than a simple chatbot. These tools can access files, interact with systems, and carry out tasks on behalf of a user, often with little supervision. Some are designed to run entirely on a local computer rather than through a browser. At the same time, more advanced models such as Claude Mythos Preview, developed by Anthropic, are showing just how powerful these systems are becoming. In controlled testing, they have been able to find weaknesses in software at a scale that was not previously possible, which is why access to them has been tightly restricted.

The key shift is simple. AI is no longer just responding to instructions. It is starting to take action.

Key Cyber Risks

1. More Ways for Things to Go Wrong. These tools often need broad access to work properly. That can include company files, emails, and connected systems. The more access something has, the more damage it can do if it is misused or goes wrong.
2. Access to Sensitive Information. Because these tools act on behalf of a user, they often inherit the same level of access. If something is misconfigured or compromised, sensitive information such as documents, passwords, or system access could be exposed.
3. Being Tricked into Doing the Wrong Thing. These tools rely on instructions and inputs, and those can be manipulated. For example, a malicious email or document could contain hidden instructions that cause the AI tool to behave in ways the user did not intend, such as sharing information or making changes.
4. Risk from Add-Ons and Integrations. Many of these tools can be extended with plugins or add-ons to increase their usefulness. However, each additional connection introduces risk. If one of those extensions is not trustworthy, it can become a pathway into the organisation.
5. Faster and More Accessible Cyber Attacks. Advanced AI models are making it easier to find and exploit weaknesses in systems. What used to take highly skilled attackers significant time can now be done faster, and potentially by less experienced individuals.

What This Means for Organisations

This shift changes how organisations need to think about risk at a practical and strategic level. End user devices are no longer just passive tools used to open documents, send emails, or access systems. They are starting to become active participants in how work is carried out, with the ability to search for information, make decisions, take action, and interact with multiple systems on a user's behalf. That creates a very different risk profile, because the device is no longer simply waiting for instructions. It may now be helping to interpret, prioritise, and carry out tasks in ways that were previously done directly by a person.

As a result, access and permissions matter more than ever. If an AI tool is installed on a local device and connected to business systems, it may be able to access the same files, messages, and services as the user. In effect, it can operate with the same authority as that individual, and in some cases at far greater speed. This means that a poor access decision, an unnecessary system connection, or an overly broad permission setting can have wider consequences than many organisations expect. What might once have been a minor oversight could now allow an AI-enabled tool to move through information, trigger actions, or expose data at scale.

At the same time, harmful activity may not look obviously malicious. One of the more difficult aspects of this risk is that the behaviour of these tools can appear entirely normal on the surface. Opening files, sending messages, searching folders, or accessing systems may all look like legitimate business activity, because in many cases they are the same kinds of actions a user would normally perform. That makes it harder for organisations to distinguish between acceptable use, poor use, manipulated behaviour, and actual compromise. In other words, the warning signs may be far less visible than in more traditional cyber incidents.

Adding to this, the speed at which cyber threats can develop and spread is increasing. AI tools can process information, carry out tasks, and respond to prompts much faster than a person. That same speed can work against an organisation if something goes wrong. A mistake, a malicious instruction, or an exploited weakness can lead to rapid consequences before staff have time to recognise the issue and intervene. This compresses response time and places greater pressure on monitoring, governance, and decision-making.

Taken together, the environment is becoming more complex and the margin for error is smaller. Organisations are not simply dealing with another software product. They are dealing with technology that can act, interact, and influence outcomes inside the business. That means cyber risk management needs to evolve accordingly, with stronger attention to oversight, access control, user awareness, and organisational readiness.

Managing the Risk

Organisations do not need to avoid these tools, but they do need to manage them carefully. The key is to treat them as powerful, high-impact software rather than everyday applications.

1. Control Where They Are Used. Not every device or user should have access to these tools. Organisations should limit their use to approved individuals or teams, maintain visibility over what tools are in use, and ensure they are reviewed before being rolled out more broadly.
2. Limit What They Can Access. These tools should only have access to what they genuinely need to perform their function. This means restricting access to sensitive files and systems, avoiding full access where partial access is sufficient, and keeping critical systems separate from general use environments.
3. Keep Them Contained. Where possible, these tools should be run in controlled environments rather than directly on a user's primary device. Using separate environments or dedicated machines helps prevent direct access to critical systems and reduces the overall impact if something goes wrong.
4. Watch What They Do. It is important to understand how these tools are being used in practice. Organisations should keep records of their activity, monitor for unusual or unexpected behaviour, and review usage regularly. This is less about detecting known threats and more about identifying behaviour that does not look right.
5. Be Careful with Add-Ons. Extensions and integrations should be tightly controlled. Only approved plugins should be allowed, their sources should be verified, and automatic installations should be avoided to reduce the risk of introducing untrusted components.
6. Build Awareness. Users need to understand that these tools can be influenced by the information they are given. External content should be treated with caution, untrusted information should not be fed into these tools, and people should be encouraged to question outputs or actions that do not seem right.
7. Update Response Plans. Organisations should be prepared for the possibility that something may go wrong. Response plans should include scenarios involving AI tools, ensure there is sufficient information available to understand what occurred, and allow for tools to be quickly disabled or isolated if required.

Closing Thought

Local AI tools are powerful, and they will become more common. They can improve productivity, but they also introduce new ways for things to go wrong. The important shift is this. Organisations are no longer just managing people and systems. They are managing software that can act on its own. That changes the risk, and it needs to be treated accordingly.

About the Bulletin:

The NZ Incident Response Bulletin is a monthly high-level executive summary containing some of the most important news articles that have been published on Forensic and Cyber Security matters during the last month. Also included are articles written by Incident Response Solutions, covering topical matters. Each article contains a brief summary and if possible, includes a linked reference on the web for detailed information. The purpose of this resource is to assist Executives in keeping up to date from a high-level perspective with a sample of the latest Forensic and Cyber Security news.

To subscribe or to submit a contribution for an upcoming Bulletin, please either visit https://incidentresponse.co.nz/bulletin or send an email to bulletin@incidentresponse.co.nz with the subject line either "Subscribe", "Unsubscribe", or if you think there is something worth reporting, "Contribution", along with the Webpage or URL in the contents. Access our Privacy Policy.

Subscribers to the premium edition also obtain access to the following additional information:

- Cyber Governance
- Cyber Incident Landscape
- Cyber Incident Response Resources
- Cyber Framework and Control Updates, Surveys and Research

Click here if you wish to subscribe to our Premium Edition of the Bulletin.

About Incident Response Solutions Limited:

Our Purpose - We help you with specialist forensic, cyber security and crisis management expertise at all stages throughout the incident response lifecycle.

Our Promise - We will provide you with the confidence you require to prepare, respond and recover from forensic and cyber incidents.

Our specialist Forensic Technology expertise includes Computer Forensics, Cybercrime Incident Response, Social Media Analysis and eDiscovery. We have significant experience in providing expert witness reports and in delivering expert witness testimony at trial. Our background includes experience in Law Enforcement (NZ Police) and Big 4 Professional Services.

Campbell McKenzie
Director
Incident Response Solutions Limited
0800 WITNESS
+64 21 779 310
campbell@incidentresponse.co.nz

Further Resources:

Alerts	Data Breach Response	Forensic Technology
Cyber Incident Simulations	Social Media Investigations	Guide for NZ Law Firms

Share our Bulletin: